JESSICA L. GRANT (SBN 178138)
JAYESH HINES-SHAH (SBN 214256)
JONATHAN A. PATCHEN (SBN 237346)
TAYLOR & COMPANY LAW OFFICES, LLP
One Ferry Building, Suite 355
San Francisco, California 94111
Telephone: (415) 788-8200
Facsimile: (415) 788-8208
E-mail: jgrant@tcolaw.com
E-mail: jhinesshah@tcolaw.com
E-mail: jpatchen@tcolaw.com

Attorneys for Defendant SOFTSCAPE, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

SUCCESSFACTORS, INC.,

Plaintiff,

v.

SOFTSCAPE, INC.,

Defendant.

Case No.: C-08-1376 (CW)

DECLARATION OF SCOTT COOPER IN SUPPORT OF DEFENDANT SOFTSCAPE, INC.'S BRIEF ADDRESSING DISCOVERY DIFFERENCES

Date: April 14, 2008
Time: N/A
Place: Courtroom 2

Honorable Claudia Wilken

I, SCOTT COOPER, declare as follows:

1. I make this declaration based on personal knowledge of the facts set forth below and on my expertise in electronic discovery and computer forensics, except for those matters that are stated on information and belief, and as to those matters I believe them to be true. If called upon to testify, I could and would competently testify thereto under oath.

2. I am a Senior Managing Director of FTI Consulting, Inc. ("FTI"). FTI is a global provider of independent forensic, technology, and consulting services, which specializes in Electronic Discovery and Computer Forensics, especially as it relates to litigation matters. (*See* www.FTIconsulting.com). I have expertise in computer systems, recovery and computer forensics. Over the last 25 years, I have performed computer consulting services for over 200 clients. Among other things, I specialize in the forensic acquisition, analysis and recovery of electronic data within and related to computer systems and electronic data and media.

3. FTI has been retained by Taylor & Company Law Offices, LLP to promptly and comprehensively assist Softscape, Inc. ("Softscape") in: (a) identifying relevant Electronically Stored Information ("ESI") that is presently known to exist within the custody and control of Softscape; and (b) preserving such evidence. FTI has been, and will continue to be, actively involved in this process.

4. Upon information and belief, to date Softscape has undertaken a number of efforts to preserve ESI, including forensic imaging of five Softscape Servers, *i.e.*, (i) the Exchange Server; (ii) the Exchange Front End Server; (iii) the Intranet Server; (iv) the Business Intelligence Server; and (v) the Server that contains all employee "home directories"; and forensic imaging of the computers of eleven (11) Softscape employees.

5. FTI's methodology for the identification, location, preservation and collection of electronic evidence is based on the internationally recognized Electronic Discovery Reference Model ("EDRM") (*see* www.EDRM.net). The EDRM protocol, an established 9-step methodology, is being followed by FTI in this matter. In pertinent part, the EDRM provides that relevant ESI should first be *identified* and *located,* and then *preserved.* As detailed below, any requirement that ESI be preserved, without the predicate prior steps of identification and location,

would depart from accepted international standards and impose an unreasonable burden upon the parties.

6. I have reviewed Softscape's proposed order to preserve evidence (the "Softscape Preservation Order"). Based on my experience in the areas of electronic discovery and computer forensics, especially as it relates to ESI, compliance with the Softscape Preservation Order is both forensically possible and feasible.

7. I have also reviewed SuccessFactors' proposed order to preserve documents (the "SuccessFactors Preservation Order") attached hereto as Exhibit 1. Based on my experience in more than 100 cases involving evidence preservation, I would find it difficult, if not impossible, to comply with Paragraph 7 of this order as drafted.

8. The SuccessFactors Preservation Order repeatedly uses undefined terms such as "logs," "metadata," and "access," each of which is susceptible to many and varied interpretations in the computer forensics field. As a result, the use of these imprecise terms makes compliance with the SuccessFactors Preservation Order infeasible.

9. Compliance with Paragraph 7 of the SuccessFactors Preservation Order, and all nine of its subsections, is, from an electronic discovery and computer forensics perspective, unreasonable and unattainable for the following reasons:

10. Subparagraph 7(a) of the SuccessFactors Preservation Order would require Softscape to preserve "all" data of the types described that "ever resided" on the Softscape intranet or other locations. This is not possible for at least two reasons. First, one cannot preserve "all" data that "ever resided" on a system. For example, data that may have resided on a system six months ago may no longer be recoverable. It is technically infeasible to capture "all" data as the SuccessFactors Preservation Order requires. Data exists in five distinct states – Live, Deleted, Slack, Unallocated, and Wiped. To gather "all" data, one would need to gather data in all five of these states, and it is simply not possible to gather artifacts from all five states of data. For example, if one forensically images a computer or server, "all" data that presently exists on that media will be preserved. That does not mean, however, that "all" data relevant to a particular document, or access to that document, has been preserved because it could have been overwritten

or deleted from the media in the normal course of business. Therefore, an order requiring a party to preserve "all" data imposes a requirement that cannot be accomplished forensically. Not only can Softscape not preserve that which has been overwritten or deleted from the media, without the creation of an entirely new system to capture and preserve ESI on a going forward basis, a party cannot literally comply with the order as drafted by SuccessFactors. Strict compliance with subparagraph 7(a) would require repeated forensic imaging on a constant basis for the duration of the case.

11. Subparagraph 7(b) of the SuccessFactors Preservation Order would require Softscape to preserve "all logs of external communications from Softscape computers over the internet, including but not limited to logs showing employees' use of third party e-mail systems ...." This subsection places no time limitations on the duty to preserve ESI relating to "logs" of external communications from Softscape computers over the Internet, regardless of the volume of data involved or whether such logs ever have existed. As stated in paragraph 8, above, in the computer forensics field the term "log" is susceptible to numerous interpretations. Further, and as stated in paragraph 10, above, it is technically infeasible to capture "all" data, with no limitation as to time, as the SuccessFactors Preservation Order requires and, as a result, compliance with this subsection of the proposed order is neither feasible nor possible from a technological standpoint.

12. Subparagraph 7(c) of the SuccessFactors Preservation Order would require Softscape to preserve "logs of dynamically (or otherwise) assigned IP addresses within Softscape." This subsection places no time limitations on the duty to preserve ESI relating to "logs" of assigned internal Softscape IP addresses, regardless of whether such logs ever have existed. In addition, compliance with this requirement of the SuccessFactors Preservation Order is not feasible because as stated in paragraph 8, above, the term "log" is susceptible to any number of interpretations in the computer forensics field.

13. Subparagraph 7(d) of the SuccessFactors Preservation Order would require Softscape to make images of every server that "ever had a copy of the Presentation or ever allowed access to the Presentation." From a technical perspective, compliance with this subparagraph of the proposed Order is infeasible because it requires a "bit-for-bit copy" or

forensic image of *any* server that *ever* allowed access to the Presentation. For instance, a server that served as a conduit and allowed data to pass through it, but never stored that data could be interpreted to have allowed "access" to the data though it would not reasonably store or house any related data. Yet the SuccessFactors Preservation Order would require Softscape to image that server. This is especially true if a party "accessed" the Presentation through the Internet, because one possible interpretation of subparagraph 7(d) would require a bit-for-bit copy of every intermediate server on the Internet, and routine Internet "transactions" often involve hundreds of separate servers. I am informed and believe, however, that the Softscape computers and servers that have been identified to date as likely to store or house ESI related to the Presentation have been forensically imaged and preserved.

14. Another concern with subparagraph 7(d) of the SuccessFactors Preservation Order is the prescribed time period (e.g., "ever had"). Preserving information throughout perpetuity is not possible with today's technology and data storage capabilities. As set forth in paragraph 10, above, it is technologically infeasible to be able to preserve, much less to know with certainty, whether any server "ever had" certain information stored therein. In addition, subparagraph 7(d) would include servers *outside* of Softscape, over which the company has no control or the ability to identify, locate or preserve evidence. As a result, I believe that compliance with subparagraph 7(d) is not feasible.

15. Subparagraph 7(e) of the SuccessFactors Preservation Order would require preservation of all e-mail boxes, repositories, archives, profiles, and calendars of a host of persons. As stated in paragraph 10, above, it is technically infeasible to capture "all" such data sources, with no limitation as to time. Moreover, given the possible number and variations of email boxes, repositories, archives, profiles, and calendars, this provision of the SuccessFactors Preservation Order is technically infeasible from a compliance standpoint. Finally, this paragraph is difficult to comply with because it mixes general terms like "executive" and specific names like "Susan Mohr."

16. Subparagraph 7(f) of the SuccessFactors Preservation Order would require preservation of "all" Softscape "e-mail distribution lists." As stated in paragraph 10, above, it is

not possible to preserve or to know with certainty that "all" such lists have been preserved with no limitations as to time, as the SuccessFactors Preservation Order would require. I am informed and believe that the Exchange Server has been identified as the likely server on which such lists would be stored or housed, and that this server has been forensically imaged and preserved.

17. Subparagraph 7(g) of the SuccessFactors Preservation Order would require preservation of logs and a forensic image of any "shared resource" ever used by Softscape executive, sales and marketing groups. This paragraph is also impracticable, from a technological perspective, because it is unclear what the term "shared resource" refers to or includes. It could be interpreted as encompassing *any* server, including an accounting server that was used by a Softscape "marketing group" to look at their payroll records. If so, this "shared resource" would have to be imaged even though that server did not contain any relevant evidence to this matter. Without further definition and some specification of the connection the resource must have to the information sought to be preserved, it would be virtually impossible to comply with this provision of the SuccessFactors Preservation Order.

18. Subparagraph 7(h) of the SuccessFactors Preservation Order would require Softscape to preserve "all VPN and FTP logs." Again, compliance with this term of the proposed order is not feasible because, as stated in paragraph 4, above, the term "log" is susceptible to many and varied interpretations in the computer forensics field. In addition, as stated in paragraph 10, above, it is technically infeasible to capture "all" data, with no limitation as to time, as the SuccessFactors Preservation Order would require.

19. Subparagraph 7(i) of the SuccessFactors Preservation Order would require Softscape to image any computer used by any person who accessed, received or communicated with anyone about the Presentation, and image every computer that ever had occasion to use one of a series of IP addresses. Compliance with subparagraph 7(i) is infeasible from a technological perspective because the term "any computer," in this context, could include an unlimited number of computers, some of which would be unknown to the user. For example, if Person A "accessed" the Presentation, and then used an accounting server to check payroll records, updated a customer database, and sent an email to schedule a medical exam, then each computer that had been "used"

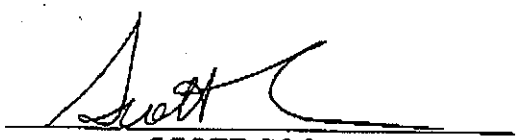
by Person A, including the accounting and customer database servers (none of which would appear relevant to this matter) would require imaging.

20. Moreover, requiring the imaging of "any" computer that "ever" used the IP addresses listed in subparagraph 7(i) of the SuccessFactors Preservation Order is technically infeasible for similar reasons. Most companies with servers or networks use computer routers that effectively "share" one IP address with hundreds, if not thousands, of computers. To the outside world, for outbound traffic, these thousands of computers all appear to be using the same IP address. However, the router handles the job of properly assigning the incoming data stream to the correct internal computers and their internal IP addresses. To the outside world, all of these computers could technically be considered to be using the same IP address. A more accessible example is the personal wireless router that many individuals now use. Although multiple persons may use the router at the same time, that router is using a solitary IP address. Yet subparagraph 7(i) would require Softscape to image *every* computer that ever used that IP address. Functionally, this would require a party to forensically image every computer that it, or any visitor, has ever used to access the Internet, and to continue to make forensic images on a constant basis for the duration of the litigation.

21. One of the most fundamental problems overall with Paragraph 7 of the SuccessFactors Preservation Order is that each of its subdivisions is inconsistent with industry practice, as reflected in the EDRM, which describes a standard and accepted methodology and protocol to work through the Electronic Discovery process, including the preservation of Electronically Stored Information. The proper protocol, which the EDRM methodology recognizes, is to identify and locate, and *then* preserve ESI. Instead, the SuccessFactors Preservation Order demands the preservation of data *before* it has been first identified, located, and shown to exist. Such an approach is extremely burdensome and does not provide for consistent and sustainable results. The EDRM does not call for the approach that is used in the SuccessFactors Preservation Order.

22. In summary, the problems presented by SuccessFactors' form of evidence preservation order, from a strictly technological compliance standpoint, are the following: (a) the order ignores the critical first steps (as outlined in the EDRM) of first *identifying* and then *locating* the data that is to be preserved; (b) the order repeatedly uses undefined and ambiguous terms to describe the data and the ESI that is to be preserved; and (c) the order is so broad in scope, and its timeline for compliance is so short that, given the available technology, it is not possible to comply fully (if at all) with the provisions as they currently are set out in the nine subsections of Paragraph 7 of the proposed order.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed this 14th day of April 2008, in Los Angeles, California.



SCOTT COOPER

EXHIBIT 1

LAURENCE F. PULGRAM (CSB NO. 115163)
lpulgram@fenwick.com
ALBERT L. SIEBER (CSB NO. 233482)
asieber@fenwick.com
LIWEN A. MAH (CSB NO. 239033)
lmah@fenwick.com
FENWICK & WEST LLP
555 California Street
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350

PATRICK E. PREMO (CSB NO. 184915)
ppremo@fenwick.com
DENNIS FAIGAL (CSB NO. 252829)
dfaigal@fenwick.com
FENWICK & WEST LLP
Silicon Valley Center
801 California Street
Mountain View, CA 94041
Telephone: (650) 988-8500
Facsimile: (650) 938-5200

Attorneys for Plaintiff
SUCCESSFACTORS, INC.

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

OAKLAND DIVISION

SUCCESSFACTORS, INC., a Delaware corporation,

Plaintiff,

v.

SOFTSCAPE, INC., a Delaware corporation; and DOES 1-10, inclusive,

Defendants.

Case No. CV 08 1376 CW

STIPULATION AND [PROPOSED] ORDER TO PRESERVE DOCUMENTS

WHEREAS, on April 1, 2008, the Court issued a written order allowing formal discovery to commence and requiring Defendant Softscape, Inc. ("Softscape") and Plaintiff SuccessFactors, Inc. ("SuccessFactors") (collectively "Parties") to confer and determine a plan for preserving electronic evidence (Docket No. 70);

WHEREAS, the Parties in this action desire to prevent spoliation or loss of evidence by clarifying certain steps that must be taken to preserve electronic data;

IT IS THEREFORE STIPULATED AND AGREED by the Parties, by and through their respective counsel of record, subject to the Court's approval, that

1. The Parties shall take reasonable steps to preserve documents, data, tangible things, and other discoverable materials within the scope of Fed. R. Civ. P. 26(b) and 34(a) that are known or reasonably likely to exist and are related to the issues presented by the action subject to the parties completing in good faith the identification of Electronically Stored Information ("ESI") that is reasonably likely be the subject of discovery in this action consistent with FRCP 26(a)(1)(B).

2. "Documents, data, tangible things, and other discoverable materials" shall include, if they exist, writings, records, files, correspondence, reports, memoranda, calendars, diaries, minutes, electronic messages (including, without limitation, chat or instant messaging), voicemail, e-mail and attachments, telephone message records or logs, electronically stored information ("ESI"), computer and network activity logs, hard drives, backup data, removable computer storage media such as PDAs, flash memory, CDs, DVDs, tapes, disks and cards, printouts, document image files, web pages, databases, spreadsheets, software, books, ledgers, journals, orders, invoices, bills, vouchers, checks, statements, itineraries, reimbursements, worksheets, summaries, compilations, computations, charts, diagrams, graphic presentations, drawings, films, digital or chemical process photographs, video, phonographic, tape or digital records or transcripts thereof, drafts, jottings and notes, whether maintained on facilities provided by a Party or not. Information that serves to identify, locate, or link such material, such as file inventories, file folders, indices and metadata, is also included in this definition.

3. "Preservation" is to be interpreted to mean accomplishing the goal of maintaining

the integrity of all documents, data, tangible things, and other discoverable materials reasonably anticipated to be subject to discovery in this action, including their metadata. Preservation means taking reasonable steps to prevent the partial or full destruction, alteration, testing, deletion, shredding, incineration, wiping, relocation, migration, theft, or mutation of such material, as well as negligent or intentional handling that would make material incomplete or inaccessible.

4. Counsel hereby confirm by their signature below that the business practices of any Party involving the routine destruction, recycling, relocation, or mutation of such materials have to the extent practicable for the pendency of this order, been revised either to:

a. Halt such business processes;

b. Sequester or remove such material from the business process; or

c. Arrange for the preservation of complete and accurate duplicates or copies of such material, suitable for later discovery if requested.

5. Counsel for the Parties hereby confirm that they have notified their clients of their document preservation obligations pursuant to federal law.

6. Counsel for Defendant shall notify New Millenium Shoe, Ely Valls, Javier Cruz, Lillian Watkins, Softscape's agents, servants, and employees, and all persons acting under, in concert with, or for Softscape that they must take all reasonable steps to locate and preserve all currently existing electronic and physical documents, things, and information that may be relevant to this dispute. Specifically, Counsel for Defendant shall notify them that they must preserve evidence concerning, at a minimum, the Presentation or communications involving New Millenium Shoe, Rick Vatcher, David Watkins, Rick Watkins, Lillian Watkins, Dennis Martinek, wildgracks@yahoo.com, William Hurley (or Hurly), williamhurly@hotmail.com, mwest@softscape.com, vallsely@hotmail.com, or hcmknowledge2008a@gmail.com.

7. With no limitation on the Softscape's obligations to preserve evidence generally, Softscape and its agents, servants, and employees, and all persons acting under, in concert with, or for them shall

a. Preserve all historical logs or metadata showing access to the Presentation, Softscape intranets, or other locations where the Presentation ever resided.

b. Preserve all logs of external communications from Softscape computers over the internet, including but not limited to logs showing employees' use of third party e-mail systems such as MSN Hotmail, Google gmail (including without limitation hcmknowledge2008a@gmail.com), and Yahoo! mail.

c. Preserve logs of dynamically (or otherwise) assigned internal IP addresses within Softscape.

d. Preserve a true, bit-for-bit copy of any server(s), including but not limited to the IIS Intranet Server, that ever had a copy of the Presentation or that allowed access to the Presentation.

e. Preserve all e-mail boxes, repositories, archives (including but not limited to .pst files), profiles, and calendars for Softscape's executives, sales teams, and other persons who accessed the Presentation, received a copy of the Presentation, or participated in communications about the Presentation, including without limitation Dave Watkins, Rick Watkins, Lillian Watkins, Susan Mohr, Dennis Martinek, Rick Vatcher, William Hurley (or Hurly), and any person using the email address mwest@softscape.com.

f. Preserve all Softscape e-mail distribution lists, including without limitation sales@softscape.com.

g. Preserve all logs of and a true copy of any shared resource used by Softscape executive, sales or marketing groups.

h. Preserve all VPN and FTP logs.

i. Make true, bit-for-bit copies of storage media of any computer (including networked storage media and home and work computers) used by persons who accessed the Presentation, received a copy of the Presentation, or participated in communications about the Presentation, including without limitation Dave Watkins, Rick Watkins, Lillian Watkins, Susan Mohr, Dennis Martinek, Rick Vatcher, William Hurley (or Hurly), and any person using the email address mwest@softscape.com, and any person using IP

addresses **98.216.168.122**, **24.34.56.79**, **82.108.171.66**, **217.118.122.88**, **62.140.137.160**, **65.96.233.62**, **65.96.237.54**, or **74.94.170.178**.

Dated: April __, 2008

FENWICK & WEST LLP

By: _____
Patrick E. Premo
Attorneys for Plaintiff SUCCESSFACTORS, INC.

Dated: April __, 2008

TAYLOR & COMPANY LAW OFFICES, LLP

By: _____
Jessica L. Grant
Attorneys for Defendant SOFTSCAPE, INC.

PURSUANT TO STIPULATION, IT IS SO ORDERED.

Dated: April ___, 2008

_____
The Honorable Claudia Wilken
United States District Court Judge

24024/00404/LIT/1283179.5